RSAC 2025 Conference

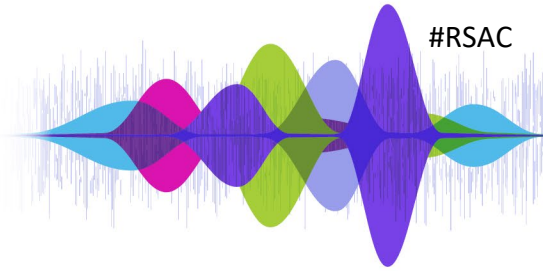
Many Voices.
One Community.

SESSION ID: HT-T10

Residential Proxies—Why Is My Cell Phone for Sale on the Dark Web?

Santiago Cortes Diaz
Director
LevelBlue

Fernando Martinez Sidera
Lead Threat Researcher
LevelBlue



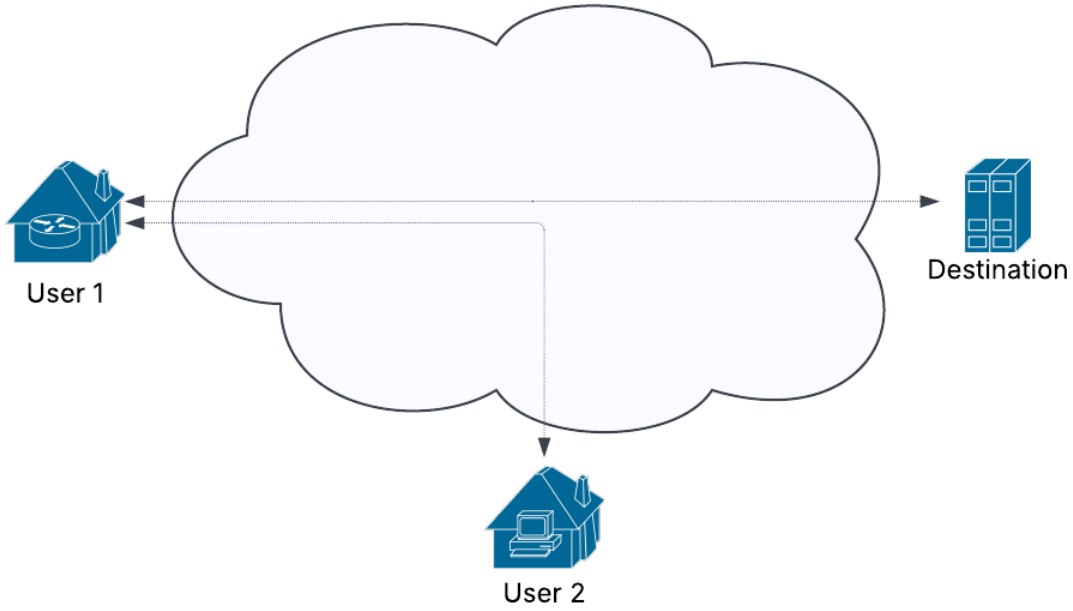
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

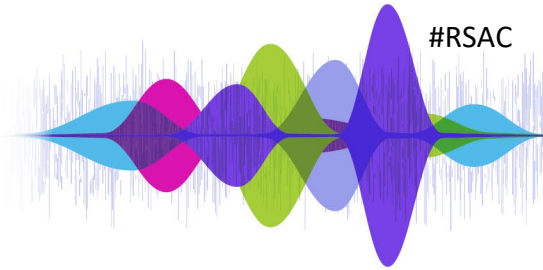
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

What are Residential Proxies?



Traditional Anonymization vs Residential Proxies



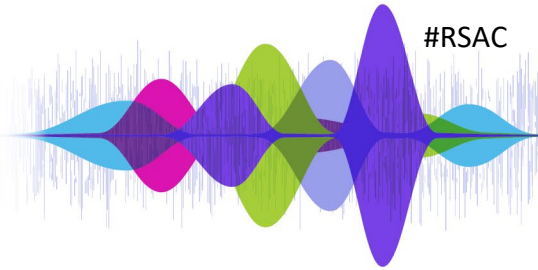
TOR/VPNs/Proxies

- Anonymized communications
- **Defenders can track assets** or providers and consider them suspicious

Residential Proxies

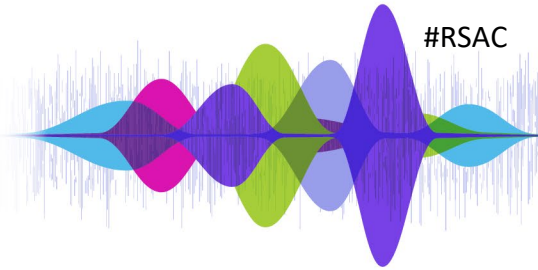
- Anonymized communications
- Proxy servers are optional
- Disposable IPs
- Proxy and user activity cannot be distinguished
- Countermeasures impact real users and customers
- Adversaries get access behind DMZ

Residential Proxies used by threat actors



- Residential Proxies for Last-Mile Access
  - APT29 leveraged residential proxies to obfuscate connections to victim environments (Mandiant, Aug 2022)
- Weaponization of Residential Proxies
  - “White Proxies” used to launch DDoS attacks against Hungarian media (Qurium, Nov 2023)
- Malware-Driven Proxy Networks
  - Malware like AdLoad (MacOS) and Mylobot (Windows) used to hijack devices and integrate them into botnets (LevelBlue, Aug 2023)

Why Residential Proxies are on the rise?



Marketing Shift: Focus on business use cases instead of anonymity

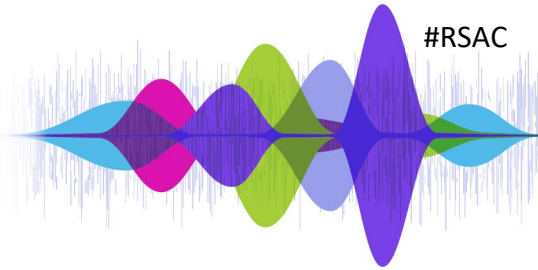
Legitimate use cases:

- Brand monitoring & Anti-counterfeiting
- SEO Monitoring
- Web Scraping

Illegitimate use cases:

- Bypassing Anti-Bot & Rate Limits
- IPTV & Streaming Services
- Adversaries operations, SPAM, DDoS
- Account Takeovers

From Underground to Mainstream

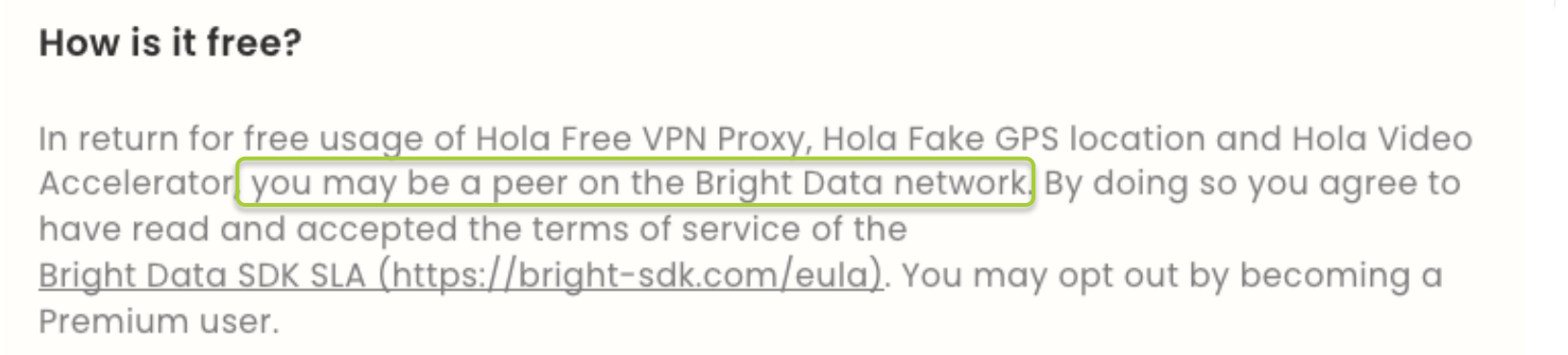


Residential proxy providers now market themselves as legitimate startups

- **Corporate Image:** Distancing from Black Market operators
- **User-Friendly Branding:** Professional websites and increased accessibility
- **Hidden Connections:** Overlapping network of residential proxy providers

Legitimate & Ethical Examples

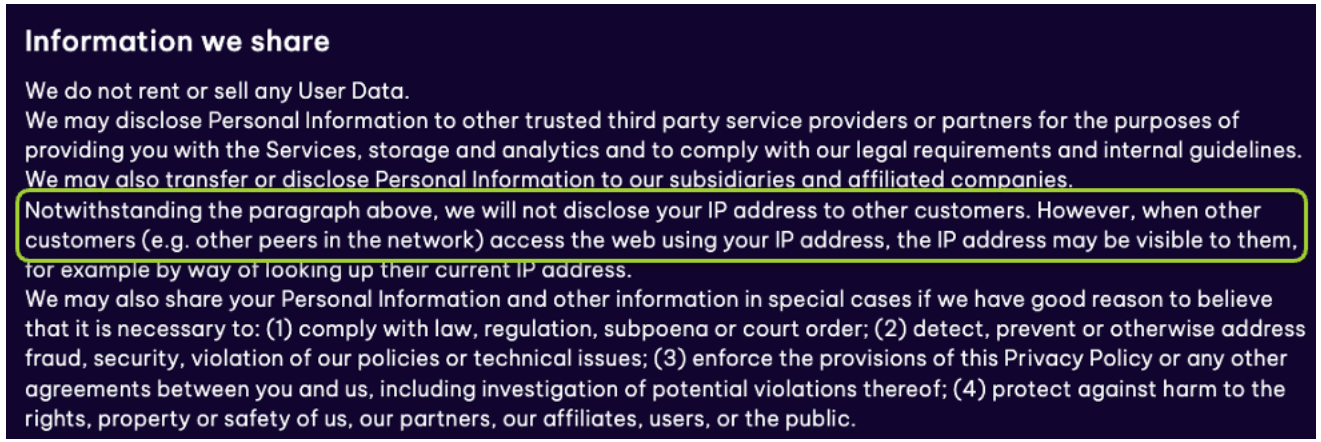
- 180 Million residential proxies
- Claim to be ethically obtained through third parties:
  - Hola VPN
  - Bright VPN
  - Pawns App
  - EarnApp…
- Starting at $4.2/GB pay per use to $2.45/GB for $12K bundles
- Different policies on Crypto



How is it free?

In return for free usage of Hola Free VPN Proxy, Hola Fake GPS location and Hola Video Accelerator you may be a peer on the Bright Data network. By doing so you agree to have read and accepted the terms of service of the Bright Data SDK SLA (https://bright-sdk.com/eula). You may opt out by becoming a Premium user.

https://hola.org/legal/sla



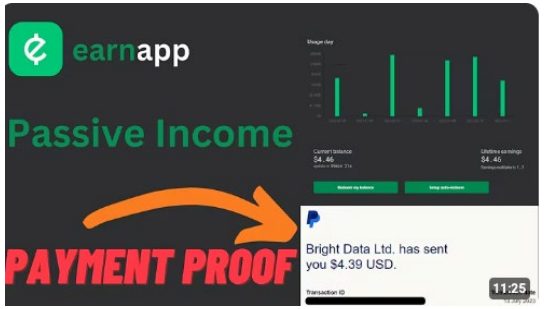
Information we share

We do not rent or sell any User Data.
We may disclose Personal Information to other trusted third party service providers or partners for the purposes of providing you with the Services, storage and analytics and to comply with our legal requirements and internal guidelines. We may also transfer or disclose Personal Information to our subsidiaries and affiliated companies.
Notwithstanding the paragraph above, we will not disclose your IP address to other customers. However, when other customers (e.g. other peers in the network) access the web using your IP address, the IP address may be visible to them, for example by way of looking up their current IP address.
We may also share your Personal Information and other information in special cases if we have good reason to believe that it is necessary to: (1) comply with law, regulation, subpoena or court order; (2) detect, prevent or otherwise address fraud, security, violation of our policies or technical issues; (3) enforce the provisions of this Privacy Policy or any other agreements between you and us, including investigation of potential violations thereof; (4) protect against harm to the rights, property or safety of us, our partners, our affiliates, users, or the public.

https://earnapp.com/privacy

Legitimate Examples – Marketing efforts

https://www.youtube.com/watch?v=pkxHqzxBB_I (Vinsane)



https://www.youtube.com/watch?v=OX_QQWK9Ais (Laurent M.)

https://www.youtube.com/watch?v=c6986UvIzJs (Mr. Money)

https://www.youtube.com/watch?v=QSxjx4Ch0rI (PaidFromSurveys)

https://www.youtube.com/watch?v=glQL_VTA_Io (Vinsane)

https://www.youtube.com/watch?v=jrFBlnc_GBA (PaidFromSurveys)

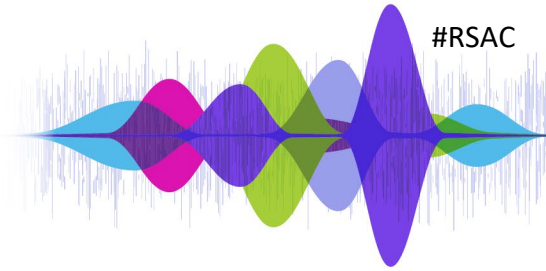
https://www.youtube.com/watch?v=7aQMj5t20UI (Christian Rauchenwald)

https://www.youtube.com/watch?v=Ryfu8ASwJAk (The Stuff)

Market competition

- Competing against backbones of millions of IPs
- Unethically obtained proxies:
  - **Easier to obtain:** Don’t always require remuneration to exit node user
  - **Competitive Pricing:** Unethically obtained proxies can be sold for a lower price
  - **Legality:** Botnet owners are not concerned for illegal activities performed by the end user
  - **Payment:** Usually paid with crypto

Resellers

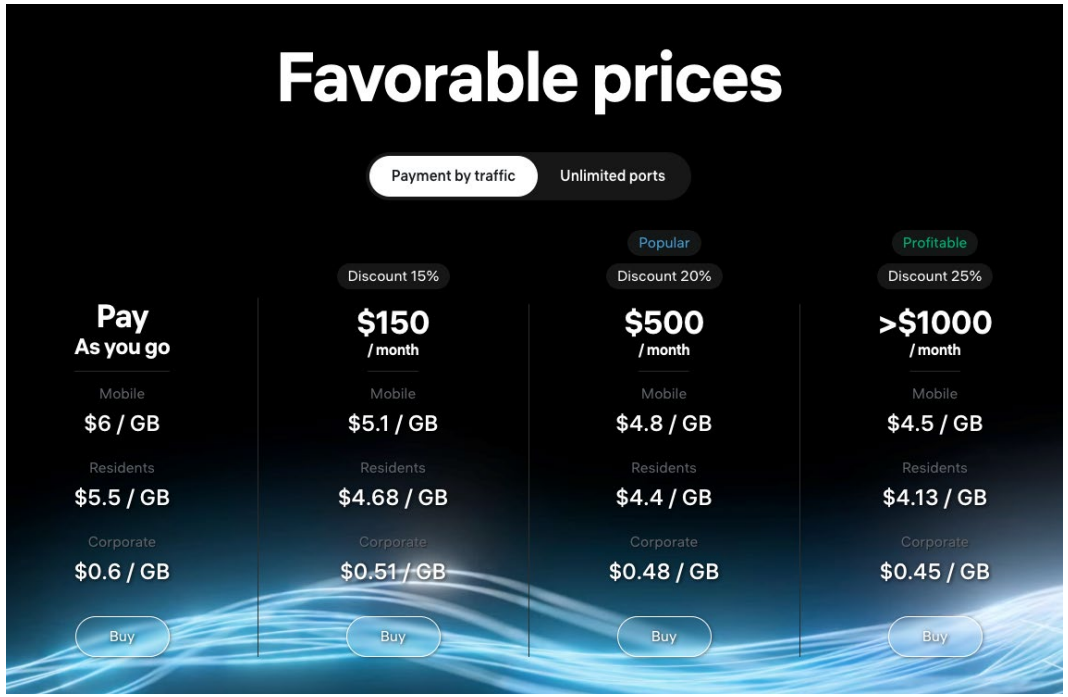


Some companies are just resellers of other residential proxy vendors.

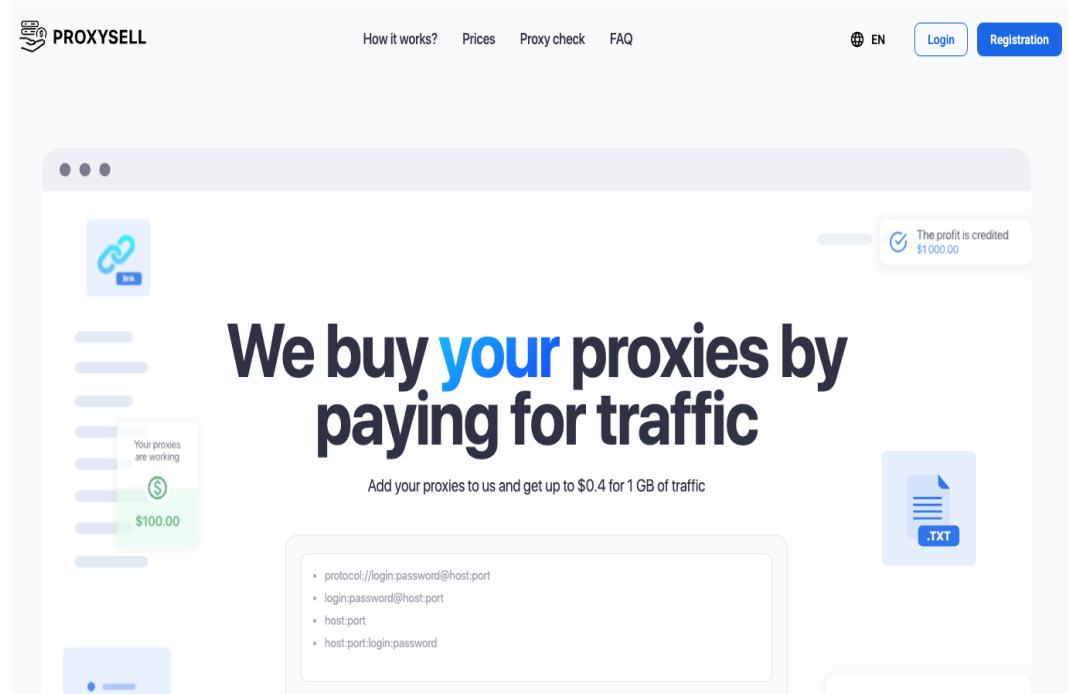
- **Lower Cost:** Buying in bulk from other vendors and combining proxies from several of them helps to offer a better starting price
- **Risk:** They don’t always ask questions of how the proxy devices were obtained.

Resellers

This company offering cellphone/residential/company proxies is located in Spain, but their home page redirects to a different domain for a company based in the British Virgin Islands:



https://sx.org/en/proxy



https://proxysell.com/en

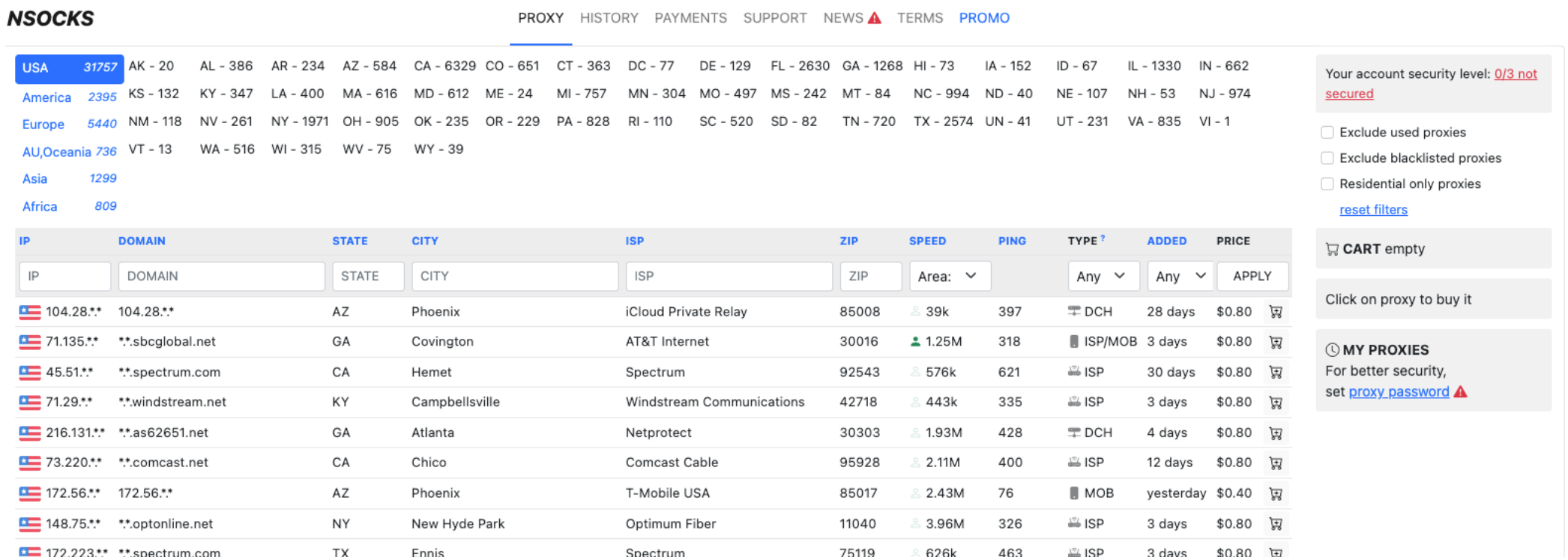
RSAC 2025 Conference

Dark Side of Residential Proxies

Nsocks

- Ngioweb botnet had scanning bots looking for vulnerable exposed systems to infect, including:
  - Routers
  - Cameras
  - Access control systems
- Infected devices ended up in Nsocks, a black-market seller
  - Main target are residential ISP users, representing over 75% of infected users
  - Prices vary between $0.20 to $1.50 for 24-hr access
  - Only allows Bitcoin or Litecoin payments

Nsocks


NSOCKS
PROXY HISTORY PAYMENTS SUPPORT NEWS TERMS PROMO
USA 31757
America 2395
Europe 5440
AU,Oceania 736
Asia 1299
Africa 809
AK - 20 AL - 386 AR - 234 AZ - 584 CA - 6329 CO - 651 CT - 363 DC - 77 DE - 129 FL - 2630 GA - 1268 HI - 73 IA - 152 ID - 67 IL - 1330 IN - 662
KS - 132 KY - 347 LA - 400 MA - 616 MD - 612 ME - 24 MI - 757 MN - 304 MO - 497 MS - 242 MT - 84 NC - 994 ND - 40 NE - 107 NH - 53 NJ - 974
NM - 118 NV - 261 NY - 1971 OH - 905 OK - 235 OR - 229 PA - 828 RI - 110 SC - 520 SD - 82 TN - 720 TX - 2574 UN - 41 UT - 231 VA - 835 VI - 1
VT - 13 WA - 516 WI - 315 WV - 75 WY - 39
Your account security level: 0/3 not secured
Exclude used proxies
Exclude blacklisted proxies
Residential only proxies
reset filters
CART empty
Click on proxy to buy it
MY PROXIES
For better security, set proxy password
IP DOMAIN STATE CITY ISP ZIP SPEED PING TYPE ADDED PRICE
Area: Any Any APPLY
104.28.*.* 104.28.*.* AZ Phoenix iCloud Private Relay 85008 39k 397 DCH 28 days $0.80
71.135.*.* *.sbcglobal.net GA Covington AT&T Internet 30016 1.25M 318 ISP/MOB 3 days $0.80
45.51.*.* *.spectrum.com CA Hemet Spectrum 92543 576k 621 ISP 30 days $0.80
71.29.*.* *.windstream.net KY Campbellsville Windstream Communications 42718 443k 335 ISP 3 days $0.80
216.131.*.* *.as62651.net GA Atlanta Netprotect 30303 1.93M 428 DCH 4 days $0.80
73.220.*.* *.comcast.net CA Chico Comcast Cable 95928 2.11M 400 ISP 12 days $0.80
172.56.*.* 172.56.*.* AZ Phoenix T-Mobile USA 85017 2.43M 76 MOB yesterday $0.40
148.75.*.* *.optonline.net NY New Hyde Park Optimum Fiber 11040 3.96M 326 ISP 3 days $0.80
172.223.*.* *.spectrum.com TX Ennis Spectrum 75119 626k 463 ISP 3 days $0.80

https://nsocks.net

Nsocks: Detection

- Two detection methods used to track it:

```
GET /metri?h=aWQ9YTM5ZWIzZWQ3OGI3NDAxZiZ2PWFybXY3bCZzdj0yNzFhJmppamNuYWRvdnFseW5nYm8= HTTP/1.1
Host: remalexation.name
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html
Connection: close
```

```
75 34.214624    8.8.8.8          192.168.2.24     DNS    460 Standard query response 0x2883 TXT enidecikive.net TXT TXT OPT
Authority RRs: 0
Additional RRs: 1
> Queries
v Answers
  v enidecikive.net: type TXT, class IN
      Name: enidecikive.net
      Type: TXT (16) (Text strings)
      Class: IN (0x0001)
      Time to live: 14334 (3 hours, 58 minutes, 54 seconds)
      Data length: 175
      TXT Length: 174
      TXT: p=hcd3QNIfLKejnBfj7Petl7D/7riIz5kfBAJGBgWdIAc4/FPgmD9R9FcaAlo/OTObpjhYDHGN7T6M1U+ixyjtcU4IgFROT/C2Bv0EGgz/ele+xqu6d984IW0EuQcQLOTLJ/F0LdLSky1soJZUc7qM6dUuLb1BTjBTZCLxBUHKfP56
  v enidecikive.net: type TXT, class IN
      Name: enidecikive.net
      Type: TXT (16) (Text strings)
      Class: IN (0x0001)
      Time to live: 14334 (3 hours, 58 minutes, 54 seconds)
      Data length: 175
      TXT Length: 174
      TXT: v=DZfEqbuLXAsGTCF96jFcrh9MLKQm4FhBTt5E3Jbk0nTg/fkNtQTwelNWjQoHuLHYeO+4ehfflOhLUVxKJKGkzOXDGjpO/hW+1bmqH6rpuReohIh16SKLZeqK6y1pxTMKaKmSzRHpwbl/uZwz2pPFmGf+Fj4kIFCWTXq1jr6Qtw==
> Additional records
[Request In: 74]
[Time: 0.006586000 seconds]
```

AdLoad & ProxyNation

AdLoad

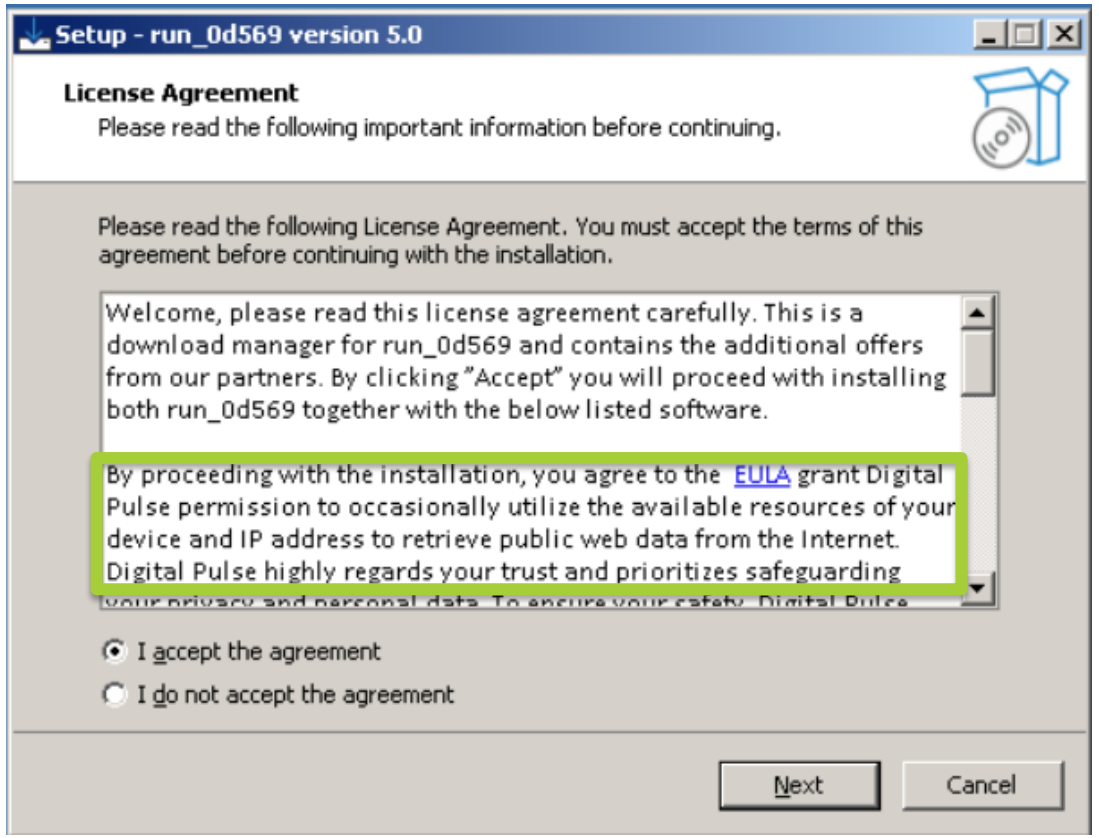
- Adware and Bundleware malware in distribution since 2017
- Behavior is similar to malware delivering Pay-Per-Install schemes.
- This campaign had matching traffic, yara and antivirus detections but carried a different payload
- Certificates and infrastructure associated with a legitimate company

ProxyNation

- Similar behavior to MacOS, but the downloader is hidden inside an executable installer for videogames and cracked software as bait
- DigitalPulseData or DigitalPulseService is repeatedly used throughout the code

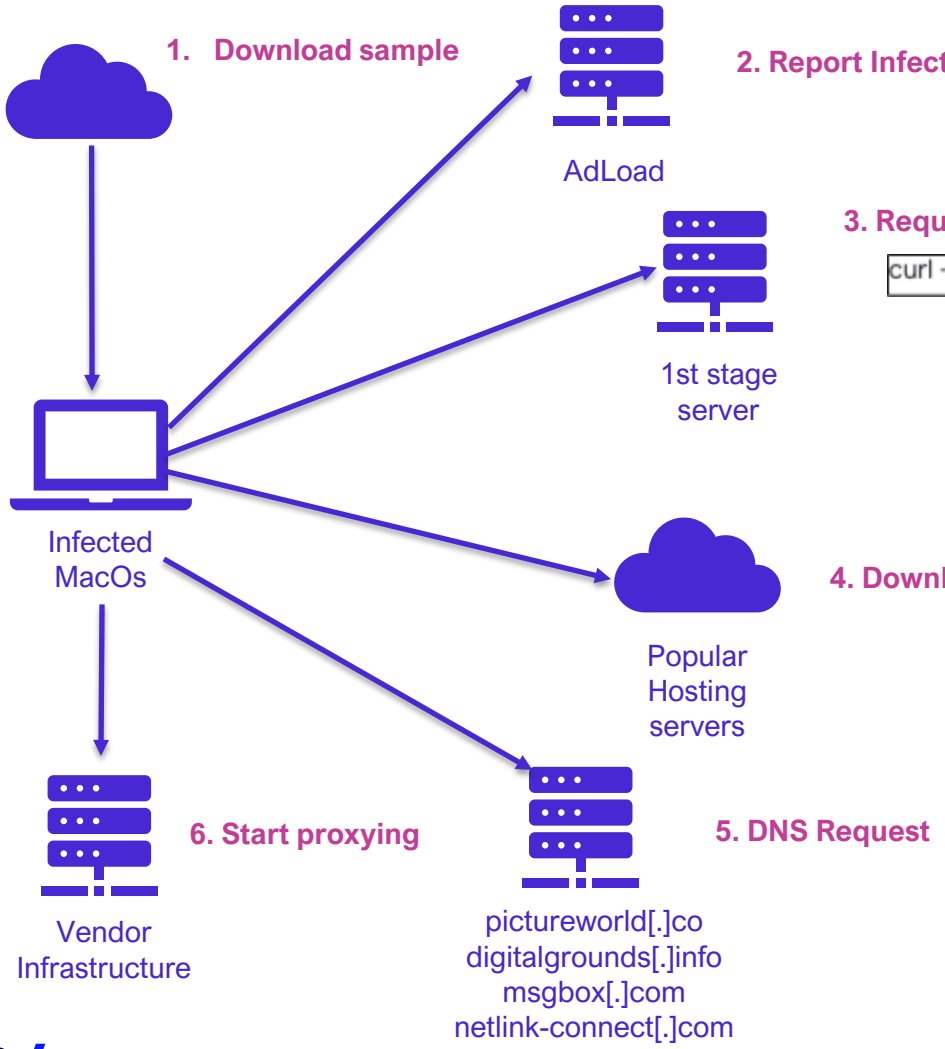
AdLoad & ProxyNation

- Company behind a P.O. Box with expired certificates
- Proxy's protocol and behavior is the same as in MacOS, and the infrastructure corresponds to the one observed with AdLoad


Setup - run_0d569 version 5.0
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Welcome, please read this license agreement carefully. This is a download manager for run_0d569 and contains the additional offers from our partners. By clicking "Accept" you will proceed with installing both run_0d569 together with the below listed software.
By proceeding with the installation, you agree to the EULA grant Digital Pulse permission to occasionally utilize the available resources of your device and IP address to retrieve public web data from the Internet. Digital Pulse highly regards your trust and prioritizes safeguarding
I accept the agreement
I do not accept the agreement
Next
Cancel

db115eff8d8b013e89f398b922294b248d5d6be51d7ab60cbde3b6ff2ff3f219

AdLoad & ProxyNation: MacOS infection



Hardcoded config:

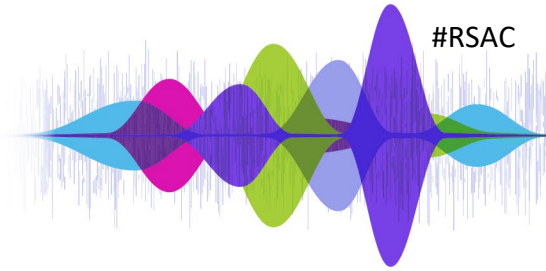

```
{"CncAddress": "papp.pictureworld.co:5000",
"CncSecurePort": 443,
"CncSsl": false,
"TrustedCAPath": "",
"BufferSize": 1024,
"ConnectionWaitSec": 60,
"Version": "0.15.31",
"LogLevel": "PROD",
"TrustedCACert": "-----BEGIN CERTIFICATE-----\nMI
```

Company N: Infrastructure

Company N: Network protocol


```
...{"peer_id":"564D2B9B-D136-1F94-5C72-8887AA0D0417","connect_version":1,"action":"connect","uuid4":"641b2dccfbb74f3e89229315338efe1a
","version":""}..h{"result":true,"error":"","action":"result","uuid4":"564D2B9B-D136-1F94-5C72-8887AA0D0417","version":""}
..d{"result":true,"error":"","action":"result","uuid4":"641b2dccfbb74f3e89229315338efe1a","version":""}GET / HTTP/1.1
Accept: application/json, text/plain, */*
User-Agent: axios/1.4.0
Accept-Encoding: gzip, compress, deflate, br
host: ip.nivadema.com
Connection: close


HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Length: 444
Content-Type: application/json
Server: workerman
Date: Thu, 15 Jun 2023 20:56:55 GMT
Connection: close

{"ip":"208.83.5.151","count":1,"country_code":"US","country_name":"United States","is_eu":false,"languages":["en-US","en"],"timezone"
:"America\/Chicago","region":null,"region_code":null,"city":null,"latitude":37.751,"longitude":-97.822,"postal":null,"asn":"AS395336"
,"isp":"MACST-ATL","vpn":false,"tor_node":false,"datacenter":false,"public_proxy":false,"web_proxy":false,"search_robot":false,"avast
el":null,"os":"macOS","timestamp":1686862615}
```

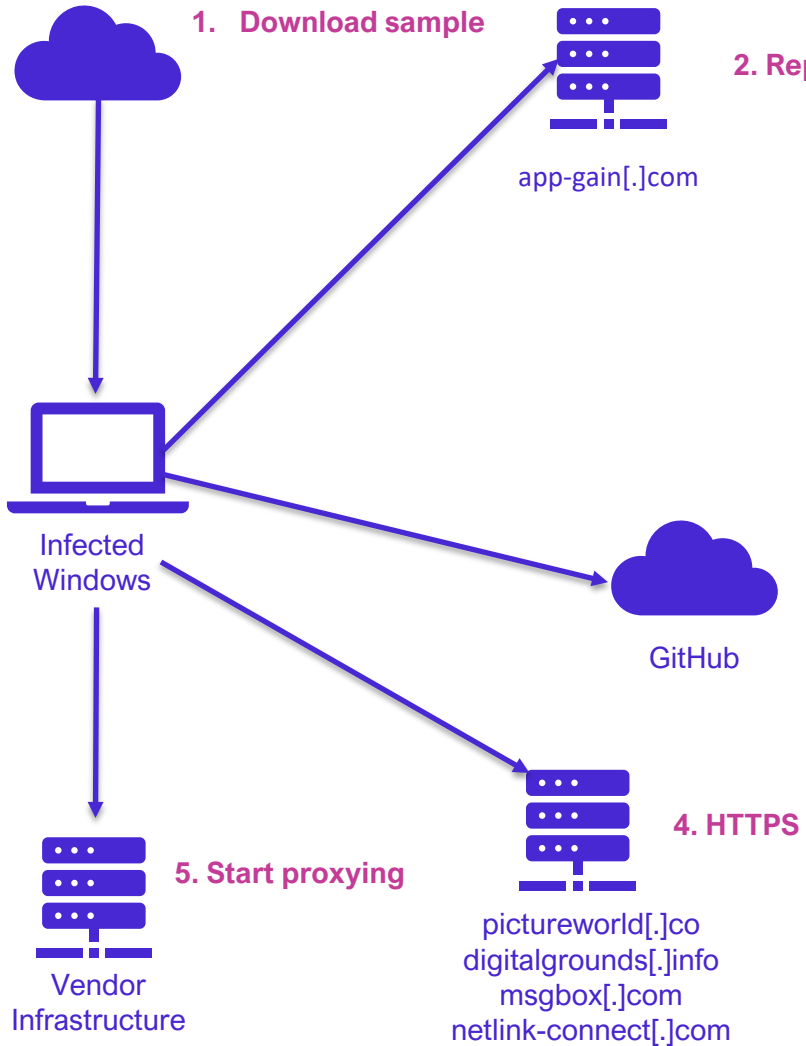
```
...{"peer_id":"564D2B9B-D136-1F94-5C72-8887AA0D0417","connect_version":1,"action":"connect","uuid4":"f69ab1
5847e44f30bf0ad568fbe145c4-10.118.0.238:7004@session@residential","version":""}..h{"result":true,"error":""
,"action":"result","uuid4":"564D2B9B-D136-1F94-5C72-8887AA0D0417","version":""}
..v{"result":true,"error":"","action":"result","uuid4":"f69ab15847e44f30bf0ad568fbe145c4-10.118.0.238:7004"
,"version":""}............n.....p.#....[.....^]..qT,.;.N. fL@..i:R1..:.~...y..bA.....VS..6. .........+./.,.
0.............../.5...uzz.......
.....................
```



Company N Response and Latest Campaign

- Company N responded to Brian Krebs that they had terminated their relationship with the publisher and banned all traffic
- Proxyware communication with Company N continues to be distributed in the form of:
  - Simple apps (AutoClicker for example) bundled with PowerShell downloaders
  - Illegal streaming apps with malicious SDKs, like:
    - Ocean Streamz
    - Flix Vision

Company N: PowerShell infection

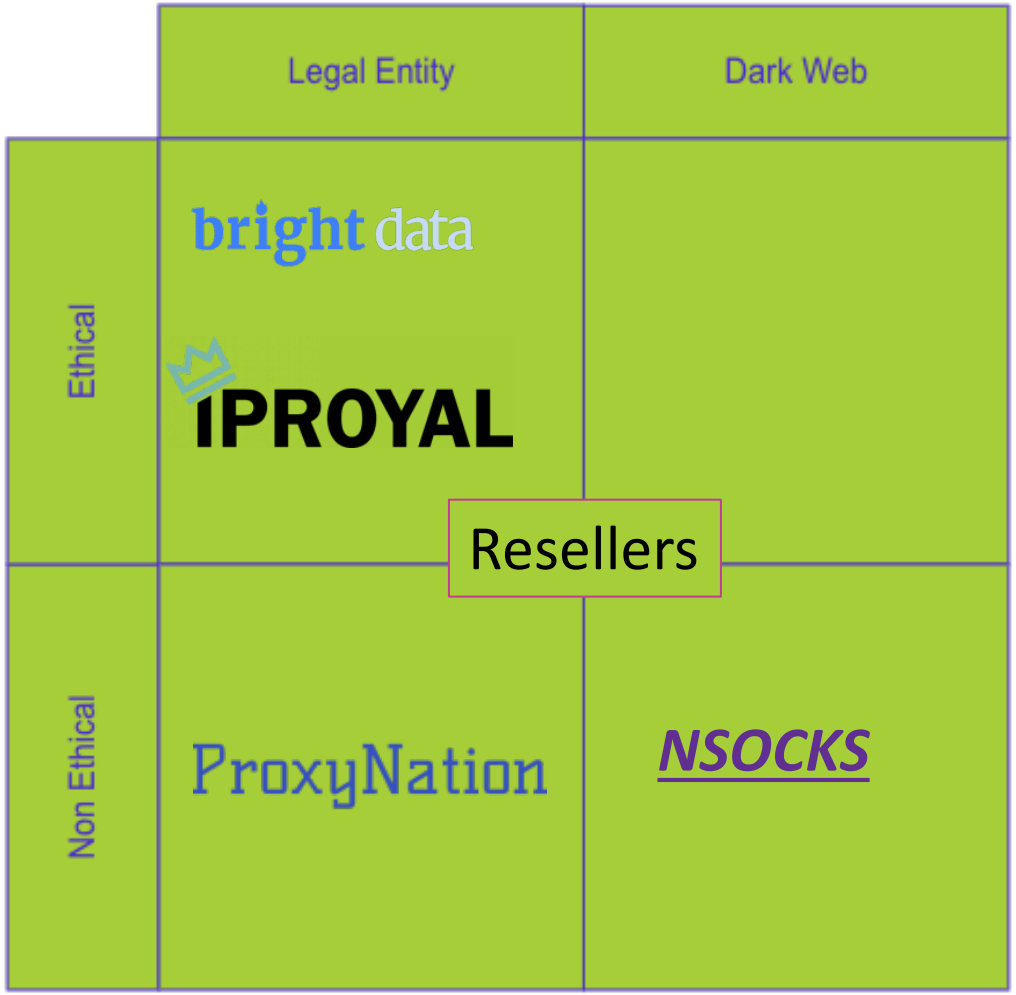


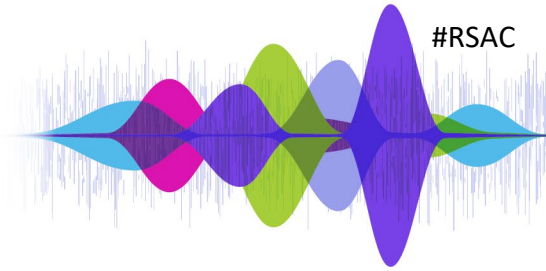

```
POST /dns-query HTTP/1.1
Host: 8.8.8.8
User-Agent: Go-http-client/1.1
Content-Length: 38
Accept: application/dns-message
Content-Type: application/dns-message
Accept-Encoding: gzip

5%..........bapp.pictureworld.co.....
```

Company N: TV SDK

Summing it up

- Residential proxies are becoming more mainstream
- Black market vendors can have tens of thousands of IPs, while legitimate entities can have millions
- Proxyware can negatively impact bandwidth
- Some providers don't encrypt traffic
- Growing concern for ISPs as vendors and companies as network consumers





Apply

Ask Questions:

- As a user, when getting free apps/money, ask yourself how is the company making money?

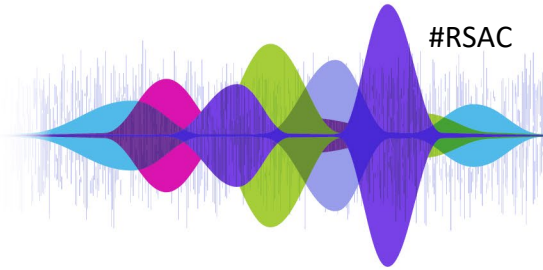
Analyze Behavior:

- Review Netflow data: Uncommon ports, traffic metrics, contacted IPs and their passive DNS
- Keep updated detections for proxyware: NIDS, yaras, AV, etc.

Apply Changes:

- Actively maintain a database/feed of malicious/undesired applications and their infrastructure
- Complement it with the use of internal/external search engines

Expectations for the future



- Residential proxies will continue growing, both legitimate and illegal.
- Different last-mile technologies will be a common TTP across adversaries.
- Adversaries will continue researching new techniques to blend in, challenging SOC teams and ML capabilities.
- Attack surface will keep increasing, outdated/EoL IoT devices all over internet will keep growing drastically.
- Exit nodes and all the providers will remain difficult to track by infrastructure/TI.
- Until more high-profile adversaries adopt them the industry will not take them seriously.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you